Remarks

Reconsideration of the subject application is requested in view of the following remarks. Claims 1-38 are in the application.

Claims 1-23 and 27-38 stand rejected as allegedly anticipated by Bernhard et al., U.S. Patent 6,275,942 ("Bernhard"). This rejection is traversed. Claim 1 recites a method for implementing an intrusion detection system in a network. The method comprises receiving a request at a software agent program to initiate intrusion detection services on a remote computer and installing intrusion detection software on the remote computer via the software agent program. The intrusion detection software is executed on the remote computer via the software agent program.

Bernhard does not teach or suggest such a method. According to Bernhard, intrusion detection systems produce a "hard coded" response to a detected intrusion. Col. 2, lines 8-15. To allow new responses to a detected intrusion, Bernhard teaches active response modules (ARMs) that can be created and installed as add-ons. Col. 3, lines 10-14. A plurality of ARMs is provided, and an appropriate ARM is invoked in response to a detected intrusion. Col. 2, lines 50-58. In contrast to Bernhard, the pending claims are directed to intrusion detection, not to responses to intrusions such as provided by Bernhard's ARMs.

According to the Office action, Bernard discloses receiving a request at a software agent program to initiate intrusion detection services on a remote compute at col. 7, lines 44-50. This portion of Bernhard does not teach or suggest receiving such a request, but instead teaches building an executable file corresponding to an ARM using a conventional "make" utility. Col. 7, lines 38-40. Installed intrusion detection system (IDS) software calls the ARM in response to detection of a particular intrusion. Col. 7, lines 48-50. The initiation of intrusion detection services in not mentioned in this portion of Bernhard.

The Office action states that Bernhard teaches installing intrusion detection software on a remote computer via a software agent program at col. 7, lines 50-65. This is incorrect. This portion of Bernhard teaches testing a newly built ARM, and preparing install and uninstall scripts for the new ARM. Installation of intrusion detection software is not mentioned.

The Office action also states that Bernhard teaches executing intrusion detection software on a remote computer via a software agent program at col. 7, lines 30-37 and col. 5, lines 8-28.

This is incorrect. The portion of Bernhard at col. 7, lines 30-37 relates to execution of code for a newly written ARM, and does not teach or suggest installation of intrusion detection software. The portion of Bernard at col. 5, lines 8-28 relates to computer networks in which intrusion detection software is provided at a central workstation, at one or more network elements, or between network elements. This portion of Bernhard does not teach or suggest remote installation of intrusion detection software via a software agent program.

For at least these reasons, claim 1 and dependent claims 2-14 are properly allowable over Bernhard.

Claim 15 recites a method for implementing an intrusion detection system on a computer connected to a network. The method includes receiving a request to become an intrusion detection platform from a remote network location, and executing the intrusion detection software in response to the request. Bernhard does not teach or suggest such a method. According to the Office action, Bernhard at col. 7, lines 44-50 teaches receiving a request to become an intrusion detection platform from a remote network location. This is incorrect. This portion of Barnard teaches building an executable file corresponding to an ARM using a conventional "make" utility. Col. 7, lines 38-40. The Office action also states that Bernhard at col. 7, lines 30-37 and col. 5, lines 8-28 teaches executing the intrusion detection software in response to the request. This is incorrect. These portions of Bernhard relates to execution of code for a newly written ARM and computer networks in which intrusion detection software is provided at a central workstation, at one or more network elements, or between network elements, respectively. Execution of intrusion detection software in response to a request to become an intrusion detection platform from a remote location is not mentioned. For at least these reasons, claim 15 and dependent claims 16-22 are properly allowable over Bernhard.

Claim 23 recites a system for detecting intrusions in a computer network, The system includes a plurality of computers executing software agents and an intrusion detection server. The intrusion detection server is configured to send a request to execute intrusion detection software to a software agent at at least one of the plurality of computers when intrusion detection services are needed based on information contained in a database. Bernhard does not teach or suggest such a network. Bernhard teaches computer networks in which intrusion detection software is provided at a central workstation, at one or more network elements, or between network elements. Col. 5, lines 8-28 and Fig. 1. Bernhard does not teach or suggest sending a

request to execute intrusion detection software, a software agent that receives such a request. For at least these reasons, claim 23 and dependent claims 24-29 are properly allowable over Bernhard.

Claim 30 recites an article of manufacture that comprises a computer-readable medium having instructions adapted to be executed by a processor. The instructions define a series of steps to be used to perform network intrusion detection that includes receiving a request at a software agent program to initiate intrusion detection services on a remote computer, and installing intrusion detection software on the remote computer via the software agent program. The intrusion detection software is then executed on the remote computer. As noted above, Bernhard does not teach or suggest receiving, at a software agent, a request to initiate intrusion detection services on a remote computer as recited in claim 30. Therefore, claim 30 and dependent claims 31-38 are properly allowable over Bernhard.

Claims 24-26 stand rejected as allegedly obvious from a combination of Bernhard and Gainsford et al., U.S. Patent 6,023,586. This rejection is traversed. Claims 24-26 are dependent from allowable clam 23 and are therefore properly allowable.

In view of the preceding remarks, claims 1-38 are in condition for allowance and action to such end is requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By _____
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446